PRIVACY IMPACT ASSESSMENT (PIA)

For the

DCPAS Defense Competency Assessment Tool (DCAT)
Defense Human Resources Activity (DHRA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☐ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☒ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 15016
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 007-000003023

~~If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.~~

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 22

DoD Component-assigned designator, not the Federal Register number.
~~Consult the Component Privacy Office for additional information or~~
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

~~or~~

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 115b, Biennial strategic workforce plan; DoD Instruction 1400.25, Volume 250, "DoD Civilian Personnel Management System: Volume 250, Civilian Strategic Human Capital Planning (SHCP)."

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of DCAT is to conduct web-based competency assessment in order to identify current and future competency gaps and requirements of the DoD civilian workforce based on near and long-term organizational goals; to support analytical reporting to Congress.

Types of personal information collected in DCAT include:
DOD ID number (EDIPI), Region ID, position ID, e-mail address, last name, first name, middle name, agency code, agency group, occupational series, organization, work City, work State, work Country, educational level, current pay plan, pay grade, pay status, supervisor status and responses to employee's and supervisor's assessment

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

There are risks that DCAT, with its extensive collection of PII, could be compromised due to unauthorized intrusion or hacking and state-sponsored information warfare. All systems are also vulnerable to "insider threats." DCAT administrators protect against this threat by limiting system access to those individuals who have a defined need to access the information. DCAT access controls limit access to the overall application and/or specific functional areas. These controls consist of privileges, general access, password control, and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which user interface features (such as buttons and menu items) are enabled for the user currently logged on. The controlled access of information to users by role ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

DCAT system administrators review audit logs periodically to ensure that data has not been created, altered, or destroyed in an unauthorized manner. The system administrators also perform quarterly information assurance (IA) and audit reviews to survey and examine records, activities, and system parameters, and to assess the adequacy of maintaining, managing, and controlling events that may degrade the security posture of the application. Security training is provided on a continuous basis to keep users alert to the security requirements. Physical controls are also in place which consist of ensuring that servers containing privileged information are housed in a secure and protected location, and limiting access to this location to individuals without a demonstrated need. An internal policy is in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within the DoD DCPAS environment, the strict security measures set by the establishment are always followed.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

DCAT receives PII from an extract from the Defense Civilian Personnel Data System (DCPDS). Participation in the competency assessment itself is voluntary, but DCAT will still include a record related to each DoD civilian employee.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Participation in the competency assessment itself is voluntary, but DCAT will still include a record related to each DoD civilian employee.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

10 U.S.C. 115b, Biennial strategic workforce plan; DoD Instruction 1400.25, Volume 250, "DoD Civilian Personnel Management System: Volume 250, Civilian Strategic Human Capital Planning (SHCP)."

PURPOSE: The information from this electronic competency assessment will be used by DoD for workforce planning and training and development purposes. Employees will rate their proficiency in a set of competencies aligned with their occupational series. Supervisors will assess their employees' proficiency level in each of these competencies and identify the target proficiency levels for the position. Supervisors and employees are encouraged to discuss the results to plan for future training and development opportunities

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Disclosure When Requesting Information Routine Use, Disclosure of Requested Information Routine Use, Congressional Inquiries, Disclosure to the Office Personnel Management Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, Disclosure to the Merit systems Protection Board Routine Use, and Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

DISCLOSURE: Voluntary. No individual administrative decisions are made based on this information; however, your responses will allow the DoD to better develop the needs of its civilian workforce.